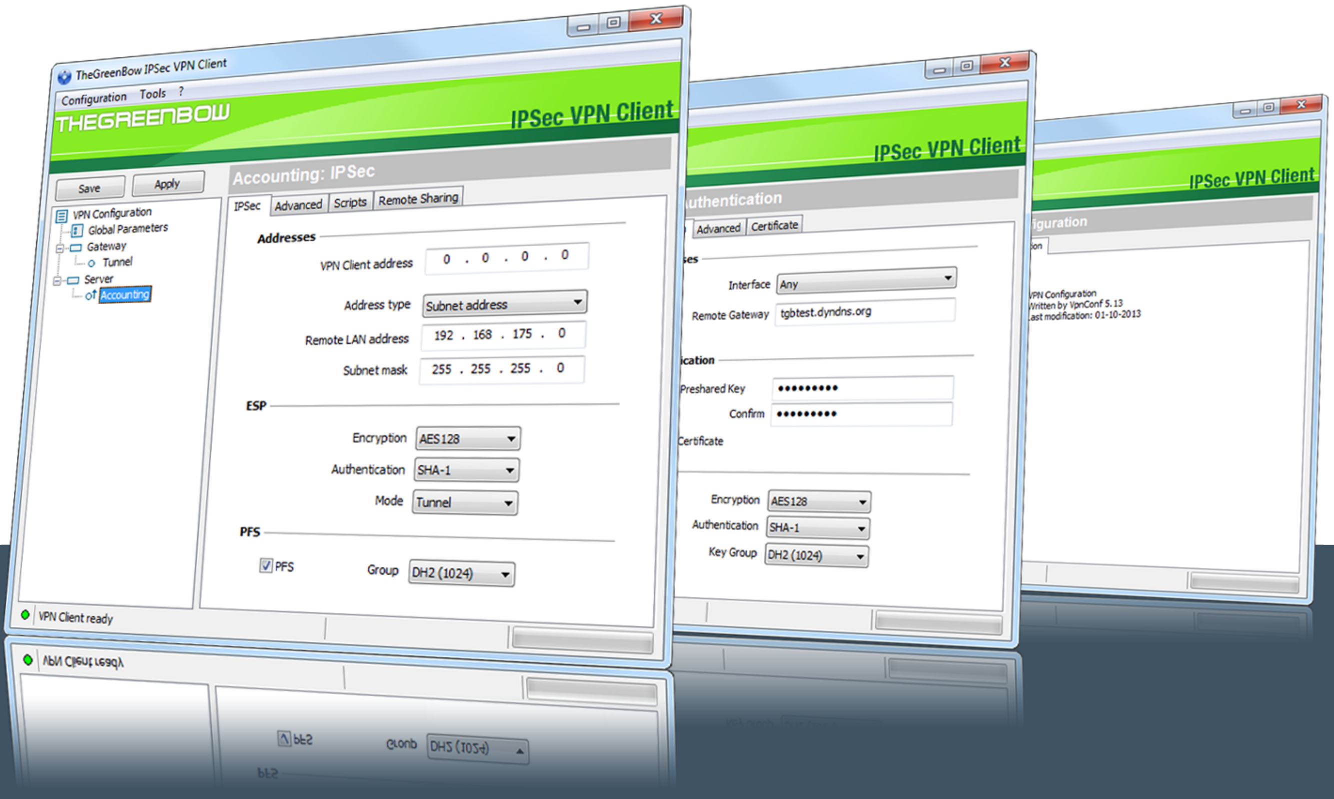


Addresses

VPN Client address 0 . 0 . 0 . 0

Address type Subnet address

Remote LAN address 192 . 168 . 175 . 0

Subnet mask 255 . 255 . 255 . 0

ESP

Encryption AES128

Authentication SHA-1

Mode Tunnel

PFS

☑ PFS Group DH2 (1024)

Interface Any

Remote Gateway tgbtest.dyndns.org

Preshared Key •••••••••

Confirm •••••••••

Encryption AES128

Authentication SHA-1

Key Group DH2 (1024)

VPN Configuration
Written by VpnConf 5.13
Last modification: 01-10-2013

TheGreenBow IPsec VPN Client

Configuration Guide
Cisco RV220W

Written by: **Anonymous Customer**

Website: **www.thegreenbow.com**
Contact: **support@thegreenbow.com**

Table of Contents

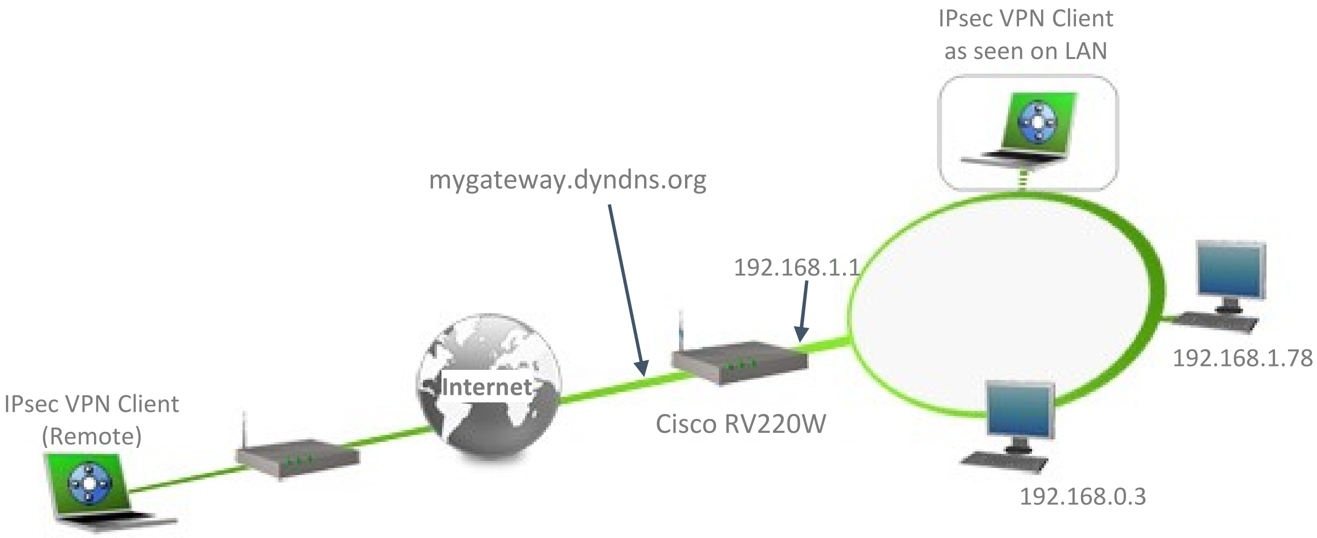
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a Cisco RV220W VPN router to establish VPN connections for remote access to corporate network.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client software to the LAN behind the Cisco RV220W router. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.



1.3 Cisco RV220W Restrictions

No known restrictions.

1.4 Cisco RV220W VPN Gateway

Our tests and VPN configuration have been conducted with Cisco RV220W firmware releases 1.0.2.4 & 1.0.4.17.

1.5 Cisco RV220W VPN Gateway product info

It is critical that users find all necessary information about Cisco RV220W VPN Gateway. All product info, User Guide and knowledge base for the Cisco RV220W VPN Gateway can be found on the Cisco website: **http://www.cisco.com/c/en/us/products/routers/rv220w-wireless-network-security-firewall/index.html**

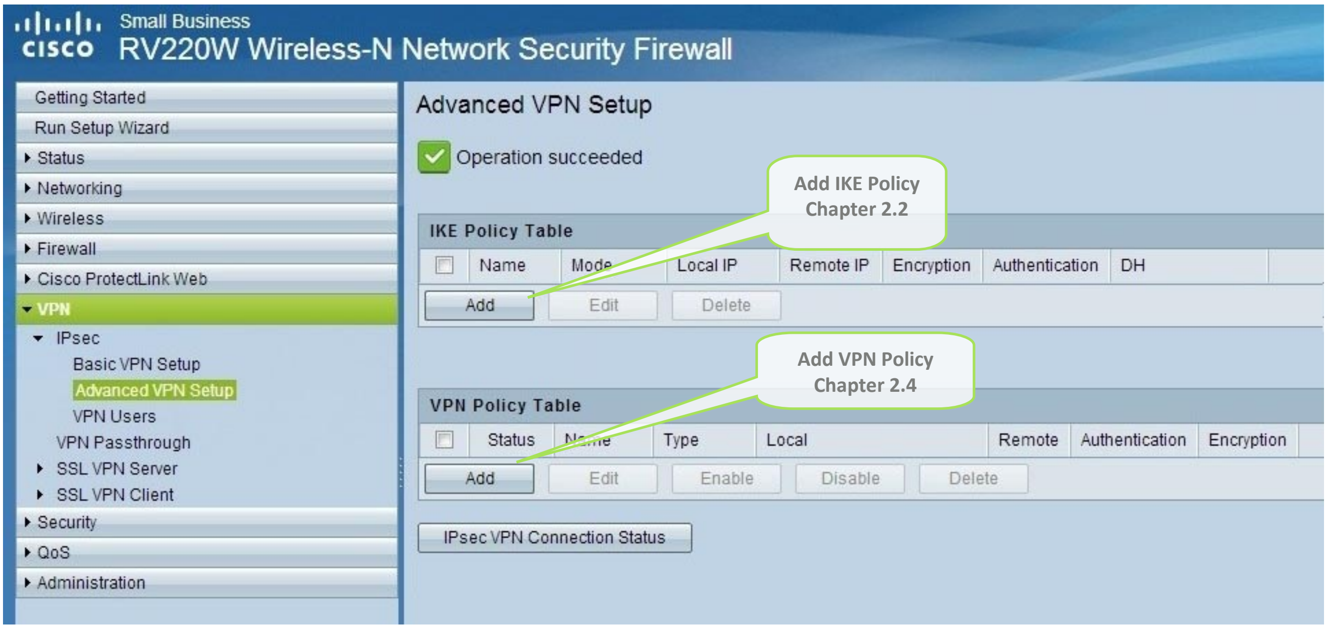
Cisco RV220W Product page	**http://www.cisco.com/c/dam/en/us/products/collateral/routers/rv220w-wireless-network-security-firewall/brochure_c02-637535.pdf**
Cisco RV220W User Guide	**http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv220w/administration/guide/rv220w_admin_v1-0-1-0.pdf**
Cisco RV220W FAQ/Knowledge Base	---

2 Cisco RV220W VPN configuration

This section describes how to build an IPsec VPN configuration with your Cisco RV220W VPN router.
Once connected to your Cisco RV220W VPN gateway,

2.1 Configure VPN using Wizard

Navigate to the menu > VPN > Advanced VPN Setup > IKE Policy Table > Add



✓ Operation succeeded

Add IKE Policy
Chapter 2.2

IKE Policy Table

□	Name	Mode	Local IP	Remote IP	Encryption	Authentication	DH

Add VPN Policy
Chapter 2.4

VPN Policy Table

□	Status	Name	Type	Local	Remote	Authentication	Encryption

2.2 Add IKE Policy

Below screenshot shows the typical settings to be used for IPSec VPN

Take note of the values set here as they would be required when configuring the TheGreenBow VPN Client. The important values include:

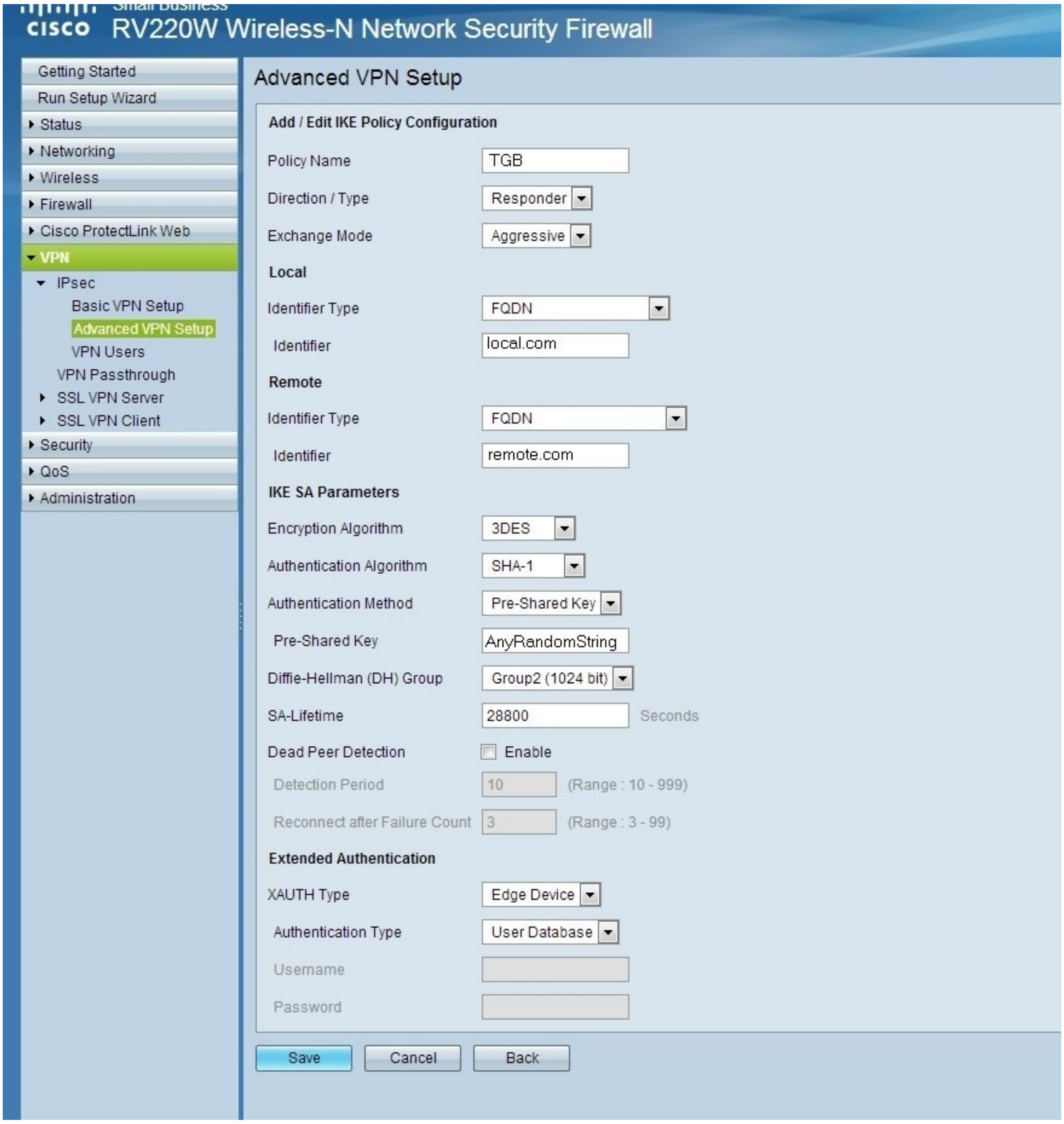
Pre-Shared Key: This can be any text string, preferably complex for security

Remote WAN IP address/FQDN: This can be remote.com or any other arbitrary value e.g. tywoddse1.com but the corresponding value used in TheGreenBow VPN Client must be the same. It does not have to be a real address i.e. resolve to a real IP address.

Local WAN IP address/FQDN: This can be local.com or any arbitrary value e.g. yywox99.com. The value does not matter, but the same value must be entered in the corresponding field in the TheGreenBow VPN Client. It does not have to be a real address i.e. resolve to a real IP address.

Local LAN IP address and subnet: This must match the LAN subnet of the Cisco RV220W router.

Click the "Save" button after entering the required information



Advanced VPN Setup

Add / Edit IKE Policy Configuration

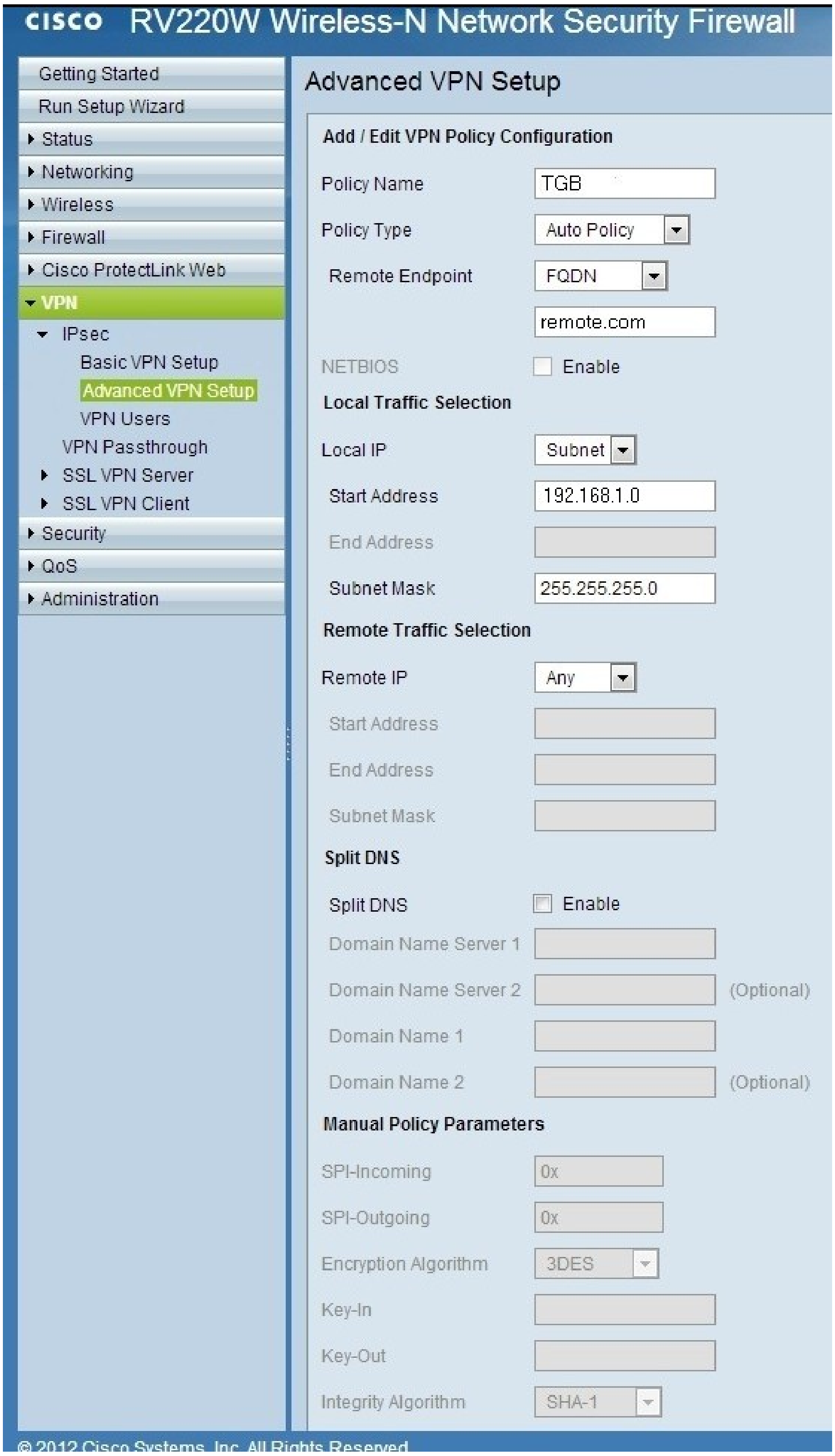
Policy Name	TGB
Direction / Type	Responder
Exchange Mode	Aggressive
Local	
Identifier Type	FQDN
Identifier	local.com
Remote	
Identifier Type	FQDN
Identifier	remote.com
IKE SA Parameters	
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	Pre-Shared Key
Pre-Shared Key	AnyRandomString
Diffie-Hellman (DH) Group	Group2 (1024 bit)
SA-Lifetime	28800 Seconds
Dead Peer Detection	□ Enable
Detection Period	10 (Range : 10 - 999)
Reconnect after Failure Count	3 (Range : 3 - 99)
Extended Authentication	
XAUTH Type	Edge Device
Authentication Type	User Database
Username	
Password	

2.3 Extended Authentication / X-Auth

Note the last set of fields in this policy:
Extended Authentication:
To use the internal user database of the Cisco Rv220w firewall set
XAUTH Type to "Edge device" and Authentication type to "User Database".

2.4 Add VPN Policy

Navigate to the menu > VPN > Advanced VPN Setup > VPN Policy Table > Add
"Select IKE Policy" links this policy to the "TGB" IKE policy.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name	TGB
Policy Type	Auto Policy
Remote Endpoint	FQDN remote.com
NETBIOS	□ Enable

Local Traffic Selection

Local IP	Subnet
Start Address	192.168.1.0
End Address	
Subnet Mask	255.255.255.0

Remote Traffic Selection

Remote IP	Any
Start Address	
End Address	
Subnet Mask	

Split DNS

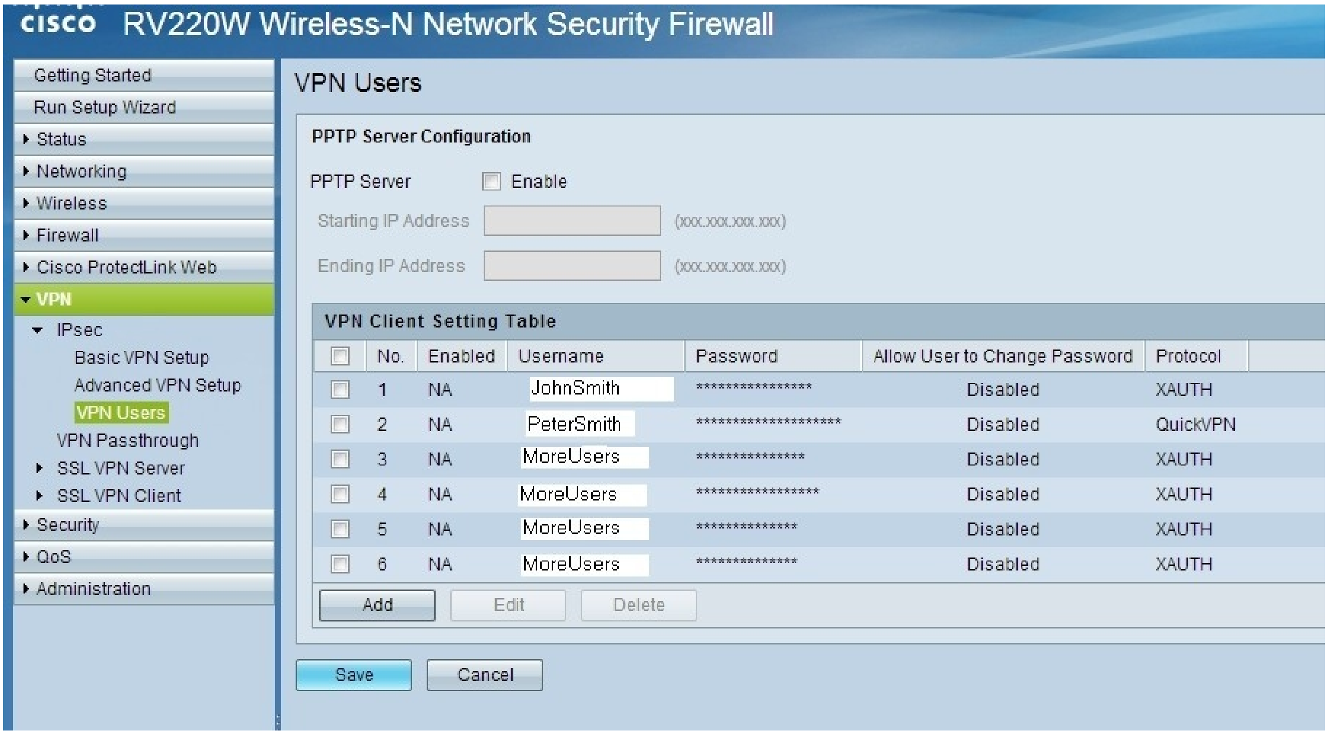
Split DNS	□ Enable
Domain Name Server 1	
Domain Name Server 2	(Optional)
Domain Name 1	
Domain Name 2	(Optional)

Manual Policy Parameters

SPI-Incoming	0x
SPI-Outgoing	0x
Encryption Algorithm	3DES
Key-In	
Key-Out	
Integrity Algorithm	SHA-1

You will need to create VPN users.
To create users, navigate go to: VPN > VPN Users

Click on Add, and then enter the username and password, and select the XAUTH protocol (for IPSec).
Take note of the username and password. This will be required when using TGB to connect



VPN Users

PPTP Server Configuration

PPTP Server □ Enable

Starting IP Address (xxx.xxx.xxx.xxx)

Ending IP Address (xxx.xxx.xxx.xxx)

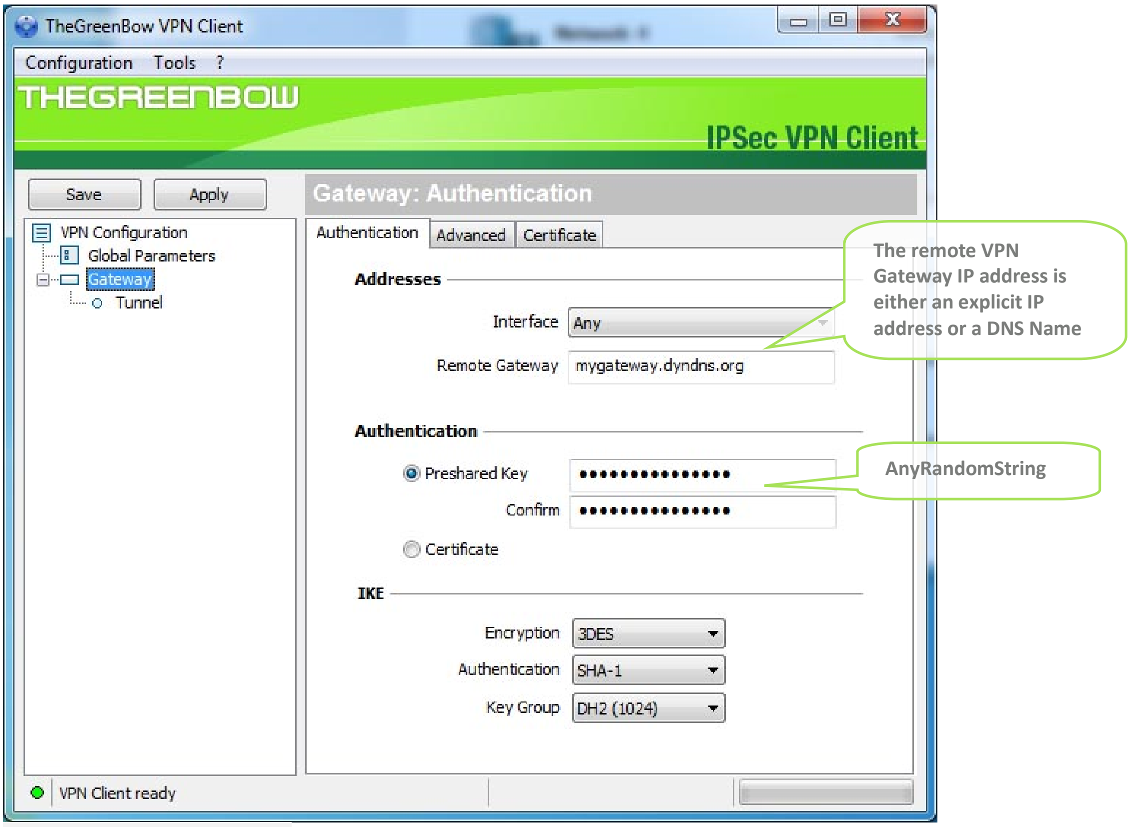
VPN Client Setting Table

□	No.	Enabled	Username	Password	Allow User to Change Password	Protocol
□	1	NA	JohnSmith	*****************	Disabled	XAUTH
□	2	NA	PeterSmith	*********************	Disabled	QuickVPN
□	3	NA	MoreUsers	****************	Disabled	XAUTH
□	4	NA	MoreUsers	******************	Disabled	XAUTH
□	5	NA	MoreUsers	***************	Disabled	XAUTH
□	6	NA	MoreUsers	***************	Disabled	XAUTH

3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a Cisco RV220W VPN router via VPN connections.
To download the latest release of TheGreenBow IPsec VPN Client software, please go to **www.thegreenbow.com/vpn_down.html.**

3.1 VPN Client Phase 1 (IKE) Configuration



Gateway: Authentication

Addresses

Interface: Any

Remote Gateway: mygateway.dyndns.org

Authentication

● Preshared Key: •••••••••••••••

Confirm: •••••••••••••••

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA-1

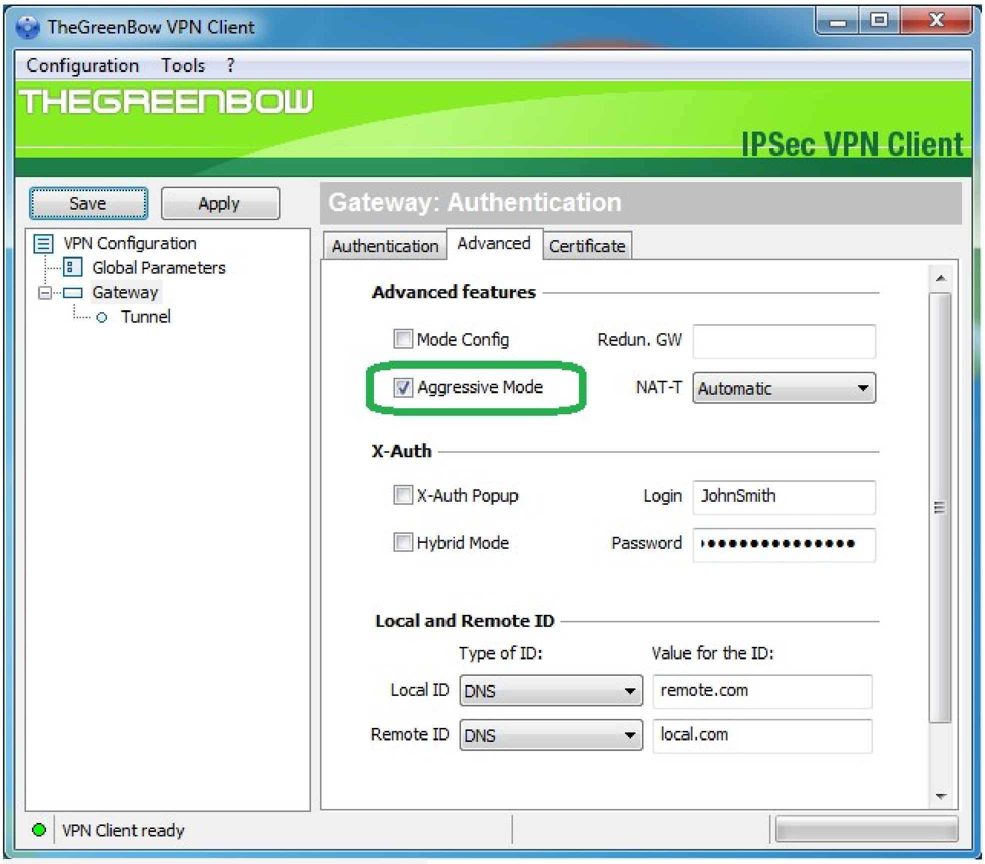
Key Group: DH2 (1024)

The remote VPN Gateway IP address is either an explicit IP address or a DNS Name

AnyRandomString

Phase 1 configuration

This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the Cisco RV220W router user guide or TheGreenBow IPsec VPN Client software User Guide for more details on User Authentication options.



☐ Mode Config

Redun. GW

☑ Aggressive Mode

NAT-T: Automatic

☐ X-Auth Popup

Login: JohnSmith

☐ Hybrid Mode

Password: •••••••••••••••

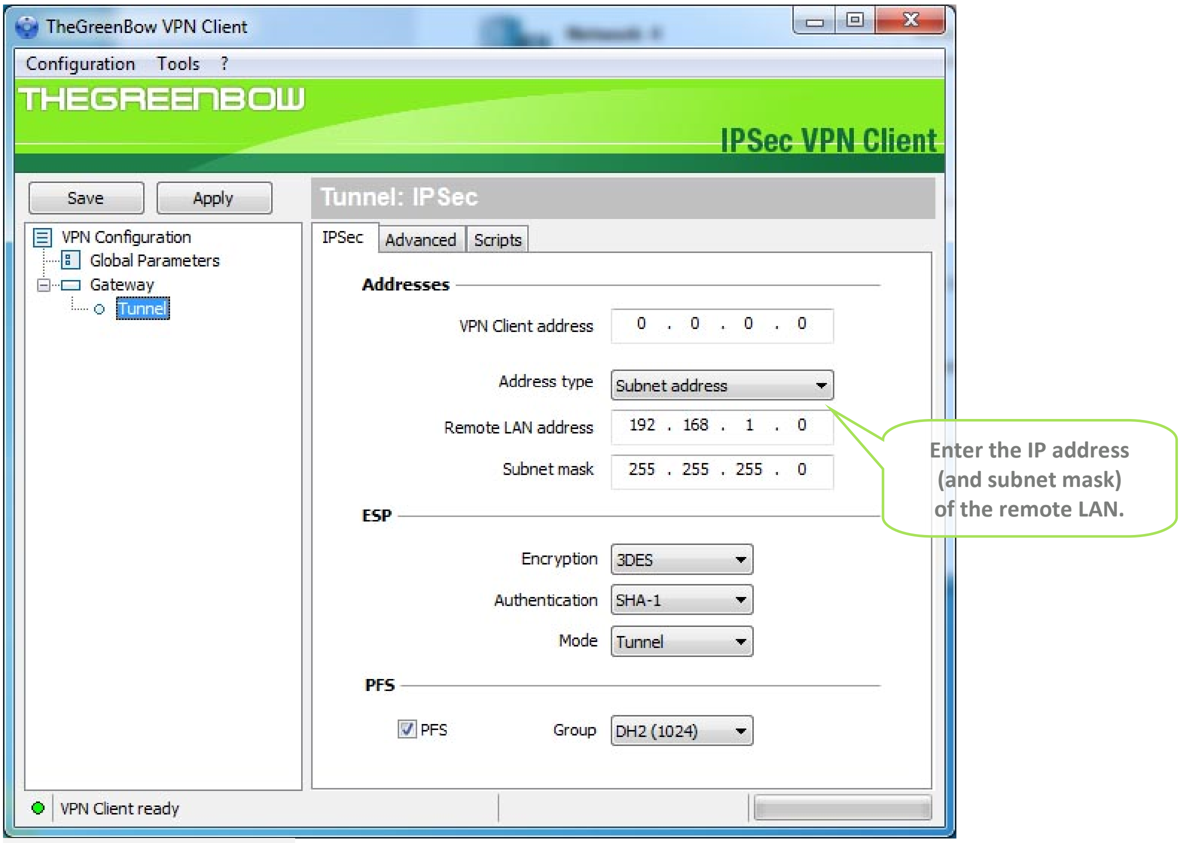
	Type of ID:	Value for the ID:
Local ID	DNS	remote.com
Remote ID	DNS	local.com

Phase 1 advanced configuration

Enable X-Auth Popup or enter X-Auth Login and Password.

Note : If X-Auth Popup is enabled, user will be requested to enter Login and Password every time the tunnel opens.

3.2 VPN Client Phase 2 (IPsec) Configuration



Tunnel: IPSec

Addresses

VPN Client address 0 . 0 . 0 . 0

Address type Subnet address

Remote LAN address 192 . 168 . 1 . 0

Subnet mask 255 . 255 . 255 . 0

ESP

Encryption 3DES

Authentication SHA-1

Mode Tunnel

PFS

☑ PFS Group DH2 (1024)

Enter the IP address (and subnet mask) of the remote LAN.

Phase 2 Configuration

3.3 Open IPsec VPN tunnels

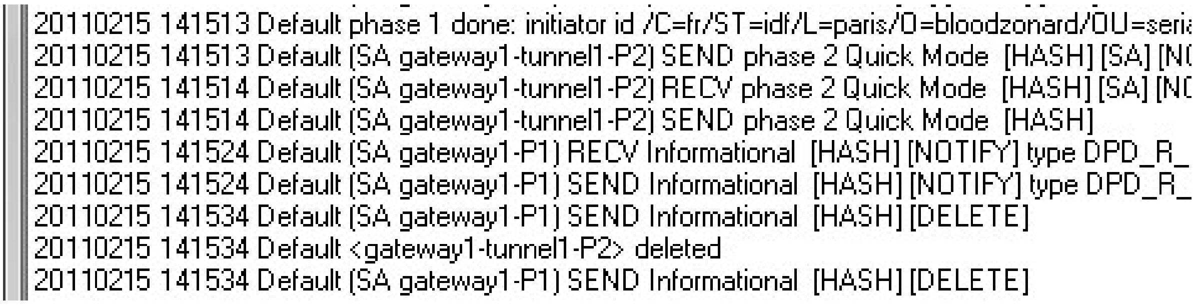
Once both Cisco RV220W router and TheGreenBow IPsec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPsec traffic.

1/ Click on "**Save & Apply**" to take into account all modifications we've made on your VPN Client configuration.

2/ Click on "**Open Tunnel**", or generate traffic that will automatically open a secure IPsec VPN Tunnel (e.g. ping, IE browser).

3/ Select "**Connections**" to see opened VPN Tunnels.

4/ Select "**Console**" if you want to access to the IPsec VPN logs and adjust filters to display less IPsec messaging. The following example shows a successful connection between TheGreenBow IPsec VPN Client and a Cisco RV220W VPN router.



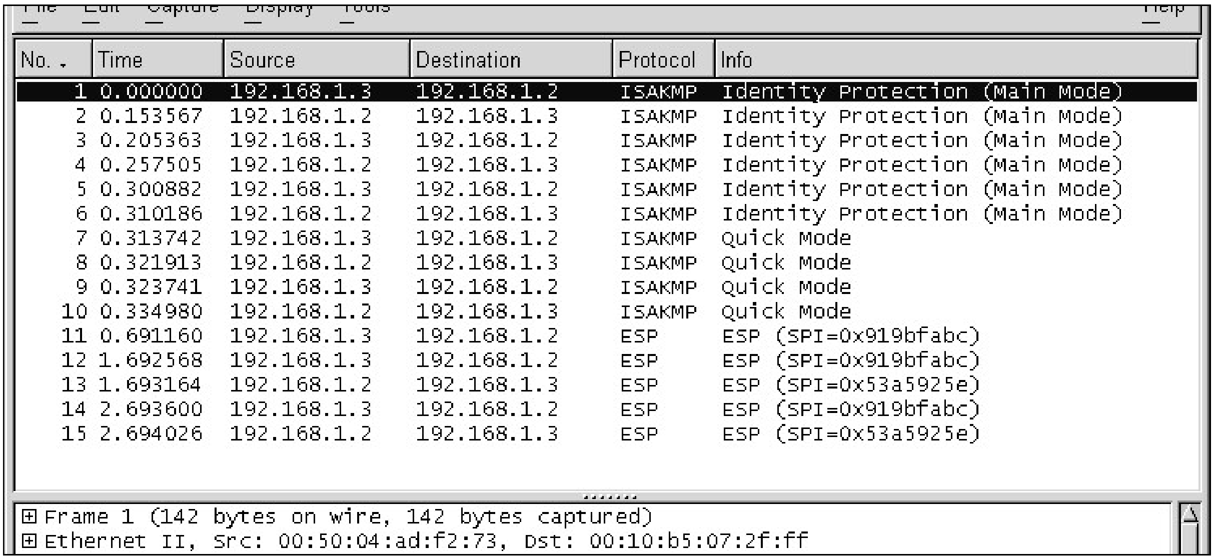
```
20110215 141513 Default phase 1 done: initiator id /C=fr/ST=idf/L=paris/O=bloodzonard/OU=seri
20110215 141513 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode  [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) RECV phase 2 Quick Mode  [HASH] [SA] [N
20110215 141514 Default (SA gateway1-tunnel1-P2) SEND phase 2 Quick Mode  [HASH]
20110215 141524 Default (SA gateway1-P1) RECV Informational  [HASH] [NOTIFY] type DPD_R_
20110215 141524 Default (SA gateway1-P1) SEND Informational  [HASH] [NOTIFY] type DPD_R_
20110215 141534 Default (SA gateway1-P1) SEND Informational  [HASH] [DELETE]
20110215 141534 Default <gateway1-tunnel1-P2> deleted
20110215 141534 Default (SA gateway1-P1) SEND Informational  [HASH] [DELETE]
```

4 Tools in case of trouble

Configuring an IPsec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

4.1 A good network analyser: Wireshark

Wireshark is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website **www.wireshark.org**. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (**www.wireshark.org/docs/**).



```
No.   Time      Source       Destination  Protocol Info
   1 0.000000  192.168.1.3  192.168.1.2  ISAKMP   Identity Protection (Main Mode)
   2 0.153567  192.168.1.2  192.168.1.3  ISAKMP   Identity Protection (Main Mode)
   3 0.205363  192.168.1.3  192.168.1.2  ISAKMP   Identity Protection (Main Mode)
   4 0.257505  192.168.1.2  192.168.1.3  ISAKMP   Identity Protection (Main Mode)
   5 0.300882  192.168.1.3  192.168.1.2  ISAKMP   Identity Protection (Main Mode)
   6 0.310186  192.168.1.2  192.168.1.3  ISAKMP   Identity Protection (Main Mode)
   7 0.313742  192.168.1.3  192.168.1.2  ISAKMP   Quick Mode
   8 0.321913  192.168.1.2  192.168.1.3  ISAKMP   Quick Mode
   9 0.323741  192.168.1.3  192.168.1.2  ISAKMP   Quick Mode
  10 0.334980  192.168.1.2  192.168.1.3  ISAKMP   Quick Mode
  11 0.691160  192.168.1.3  192.168.1.2  ESP      ESP (SPI=0x919bfabc)
  12 1.692568  192.168.1.3  192.168.1.2  ESP      ESP (SPI=0x919bfabc)
  13 1.693164  192.168.1.2  192.168.1.3  ESP      ESP (SPI=0x53a5925e)
  14 2.693600  192.168.1.3  192.168.1.2  ESP      ESP (SPI=0x919bfabc)
  15 2.694026  192.168.1.2  192.168.1.3  ESP      ESP (SPI=0x53a5925e)

⊞ Frame 1 (142 bytes on wire, 142 bytes captured)
⊞ Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff
```

5 VPN IPsec Troubleshooting

5.1 “PAYLOAD MALFORMED” error (wrong Phase 1 [SA])

```
114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [NOTIFY]
114920 Default exchange_run: exchange_validate failed
114920 Default dropped message from 195.100.205.114 port 500 due to notification type
PAYLOAD_MALFORMED
114920 Default SEND Informational  [NOTIFY] with PAYLOAD_MALFORMED error
```

If you have an “PAYLOAD MALFORMED” error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 “INVALID COOKIE” error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105
115933 Default dropped message from 195.100.205.114 port 500 due to notification type
INVALID_COOKIE
115933 Default SEND Informational  [NOTIFY] with INVALID_COOKIE error
```

If you have an “INVALID COOKIE” error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

5.3 “no keystate” error

```
115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115319 Default IPsec_get_keystate: no keystate in ISAKMP SA 00B57C50
```

Check if the preshared key is correct or if the local ID is correct (see “Advanced” button). You should have more information in the remote endpoint logs.

5.4 “received remote ID other than expected” error

```
120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
120351 Default ike_phase_1_recv_ID: received remote ID other than expected
support@thegreenbow.fr
```

The “Remote ID” value (see “Advanced” Button) does not match what the remote endpoint is expected.

5.5 “NO PROPOSAL CHOSEN” error

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72:
195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
115915 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode  [SA][KEY][ID][HASH][NONCE]
115915 Default RECV Informational  [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error
115915 Default RECV Informational  [HASH][DEL]
115915 Default CNXVPN1-P1 deleted
```

If you have an “NO PROPOSAL CHOSEN” error, check that the “Phase 2” encryption algorithms are the same on each side of the VPN Tunnel.

Check “Phase 1” algorithms if you have this:

```
115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
115911 Default RECV Informational  [NOTIFY] with NO_PROPOSAL_CHOSEN error
```

5.6 “INVALID ID INFORMATION” error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode  [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72:
195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
122626 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode  [SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational  [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational  [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

If you have an “INVALID ID INFORMATION” error, check if “Phase 2" ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type (“Subnet address” and “Single address”). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

5.7 I clicked on “Open tunnel”, but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPsec Client uses UDP port 500 and protocol ESP (protocol 50).

5.8 The VPN tunnel is up but I can't ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP
- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark for example). You will have an indication that encryption works.
- Check the "default gateway" value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no "Default gateway" setting.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- We recommend you to install Wireshark (**www.wireshark.org**) on one of your target computer. You can check that your pings arrive inside the LAN.

6 Contacts

News and updates on TheGreenBow web site: **www.thegreenbow.com**

Technical support by email at: **support@thegreenbow.com**

Sales contacts by email at: **sales@thegreenbow.com**

Secure, Strong, Simple

TheGreenBow Security Software